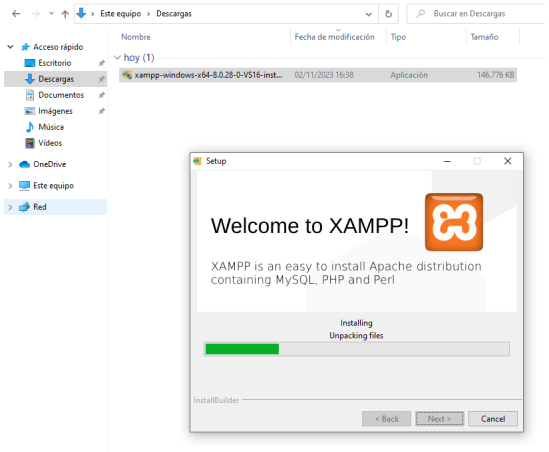
EXAMEN UNIDAD 1 – EJERCICIO NMAP

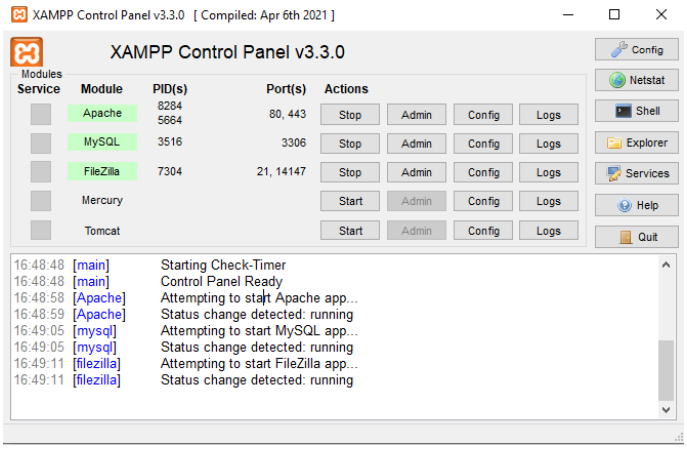
2º SMR – IES RAMÓN M.ª ALLER ULLOA

Nicolás González Dobarro

Índice

1. Instala XAMPP en Windows e inicia los servidores Apache, MySQL y FileZilla.





2. Escanea la máquina Windows desde Ubuntu con NMAP (usando la interfaz de consola).

1. Identifica qué servicios están disponibles en la máquina Windows.

Usamos el comando nmap -sV 172.16.224.4 (IP cliente Windows) y nos proporciona todos los servicios con sus respectivas versiones que están corriendo en Windows.

```
root@usuario: /home/nicolas
root@usuario:/home/nicolas# nmap -sV 172.16.224.4
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-02 16:50 CET
Nmap scan report for 172.16.224.4
Host is up (0.00023s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
80/tcp   open  http          Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MariaDB (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:CD:F6:0A (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.64 seconds
root@usuario:/home/nicolas#
```

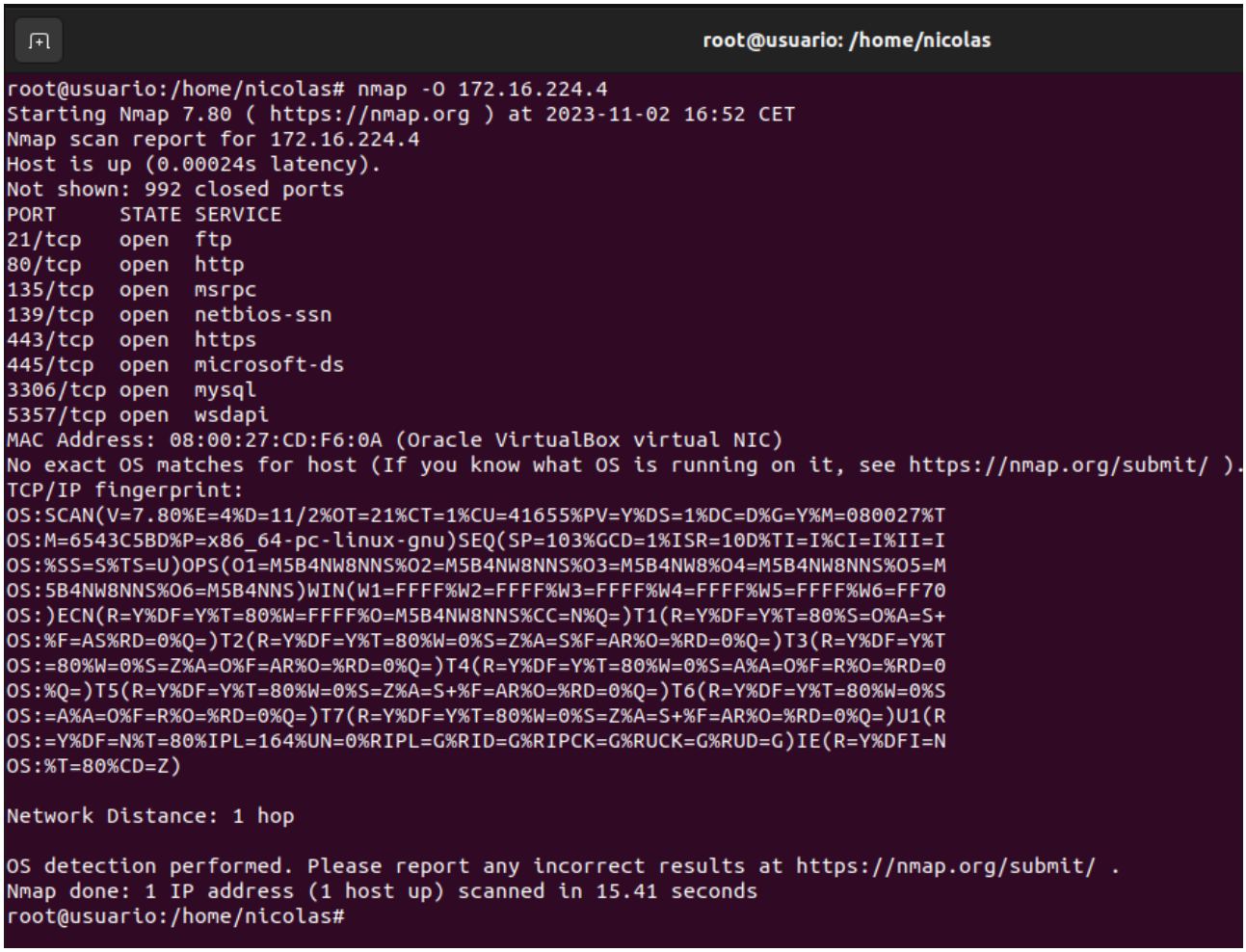
2. ¿Cuáles son las versiones de los servicios activos?

El comando utilizado es el mismo que el del ejercicio anterior.

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
80/tcp   open  http          Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MariaDB (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

3. Ejecuta las opciones adecuadas para identificar el sistema operativo de la máquina objetivo.

Utilizamos el comando nmap -O 172.16.224.4, en el cual -O es el parámetro para comprobar el sistema operativo de dicha IP. No nos proporciona ningún S.O. debido a un error porque tiene muchas etiquetas.



3. Escanea desde Windows toda la red con NMAP (usando la interfaz gráfica) para comprobar los hosts activos.

1. Muestra la imagen de toda la red.

Usamos el comando nmap -T4 -F 172.16.224.0/24, indicando la dirección de red y máscara para que nos muestre todos los equipos encendidos de esa red. Podemos observar que están disponibles el 172.16.224.2 y 172.16.224.4, los cuales son Ubuntu y Windows respectivamente.